AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched

a. White apple iPhone with gold cover (hereinafter Target Device #1)
b. Blackberry cellular telephone model REY21CW (hereinafter Target Device #2)
CURRENTLY LOCATED AT DAYTON RESIDENCE OFFICE, DEA, 3821 COLONEL GLENN HIGHWAY, BEAVERCREEK, OH

Case No. 3:19mj052

MICHAEL J. NEWMAN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1956(h)	Conspiracy to commit money laundering.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO STEVE DUTEIL, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: February 4, 2019

Judge's signature

City and state: DAYTON, OHIO

MICHAEL J. NEWMAN, U.S. MAGISTRATE JUDGE
Printed name and title

ATTACHMENT A

The property to be searched is:

a. White apple iPhone with gold cover (hereinafter Target Device #1)

b. Blackberry cellular telephone model REY21CW (hereinafter Target Device #2)

(collectively referred to as **Devices**).

The Devices are currently located at the Dayton Residence Office, Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, OH.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of **18 U.S.C. 1956(h) (conspiracy to commit money laundering)** and involve **Moises Gonzalez, Jr. and Jason Thomas** since **January 2016** including:

   a. Contracts and arrangements for the delivery of bulk cash and wiring of money;

   b. any information related to sources of money (including names, addresses, phone numbers, or any other identifying information);

   c. lists of customers and related identifying information;

   d. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   e. any information recording **Jason Thomas**'s schedule or travel from **January 2016** to September 30, 2016;

   f. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:

a. White apple iPhone with gold cover (hereinafter Target Device #1)

b. Blackberry cellular telephone model REY21CW (hereinafter Target Device #2)

CURRENTLY LOCATED AT DAYTON RESIDENCE OFFICE, DEA, 3821 COLONEL GLENN HIGHWAY, BEAVERCREEK, OH

3:19mj052

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Steven V. Duteil, Task Force Officer of the Drug Enforcement Administration, United States Department of Justice, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the Drug Enforcement Administration, and have been since August 25, 2014. Your affiant worked as a uniformed Ohio State Patrol (OSP) Trooper from 1993 until 2009, and was subsequently transferred to the Office of Investigative Services (OSP) section until 2011. In 2011, your affiant was promoted to Sergeant, and was

transferred to the Springfield Post of the Ohio State Patrol. During this time period, your affiant has conducted numerous narcotic related investigations involving illegal narcotics; and prepared and executed search warrants for locations where cocaine, marijuana, heroin, and prescription pills were stored/distributed. Your affiant has conducted investigations into conspiracy to convey narcotics into state owned facilities; unlawful possession, possession with the intent to distribute, and the actual distribution of controlled substances, in violation of Title 21, United States Code, Sections 841(a)(1) and 846. Your Affiant has also been involved with the administrative duties and monitoring responsibilities of Title III wire intercepts, and analysis of pen registers related to narcotics and gang investigations. Your Affiant is familiar with their methods of concealing the whereabouts of illegal drugs, the methods used to keep law enforcement officers from finding evidence of drug trafficking operations, as well as the methods used to prevent others unfamiliar with criminal conduct from observing things indicative of drug trafficking. Your Affiant is also familiar with the paranoia surrounding most drug traffickers and the common ways in which wholesale drug distributors attempt to conceal their assets, their purchases, and other financial dealings that could be traced to them.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PURPOSE OF THE AFFIDAVIT

4. Your Affiant makes this affidavit in support of applications for search warrants for the below listed devices, as there is probable cause to believe that evidence of a crime, contraband, or fruits of a crime, and property designed for use, intended for use, or used in

committing a crime—namely, violations of 18 U.S.C. 1956(h) (conspiracy to commit money laundering) – exists and can be found on the following devices:

a) White apple iPhone with gold cover (hereinafter Target Device #1)

b) Blackberry cellular telephone model REY21CW (hereinafter Target Device #2)

(collectively referred to as **Devices**).

5. The Devices are currently located at the Dayton Residence Office, Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, OH.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. Between 2013 and 2017, the Boston Field Division of the Drug Enforcement Administration targeted a money launderer broker based in Cucuta, Colombia. Members of Colombian drug trafficking organizations employed this money launderer broker to coordinate the pick-up of bulk cash in the United States and its wiring to specific bank accounts both in the United States and abroad. The Colombian drug trafficking organizations would pay the money launderer broker in return for arranging these pick-ups and deliveries a percentage of the money delivered. The money was believed to be drug proceeds.

8. In turn, the money launderer/broker employed another broker (in this investigation, a U.S. undercover law enforcement agent ("UC-1")) to arrange the specific details of the pick-up of the bulk cash in the United States. The money launderer broker would pay UC-

1 in return for arranging these pick-ups and deliveries a percentage of the money delivered. UC-1 regularly communicated with the money launderer broker via text message on a Blackberry device.

9. When UC-1 accepted a contract to pick-up bulk cash from the money launderer broker, UC-1 would provide the telephone number for a third-party courier (in this investigation, a U.S. undercover law enforcement agent would play the part of this "third party," hereinafter tasked with picking up the bulk cash. The co-conspirator tasked with dropping off the bulk cash on behalf of the Colombian drug trafficking organization would contact the third party courier to arrange the specifics of the delivery of the bulk cash.

10. To ensure that the bulk cash was delivered to the correct person, a pre-arranged code was used. The person picking up or taking physical custody of the bulk cash would provide a photograph of a serial number from a specific dollar bill (paper currency) in his possession to UC-1 who passed this serial number onto the money launderer broker. The money launderer broker would give this serial number to the person delivering the cash. At the time of the delivery of the cash, the person dropping off the cash would give the serial number provided to him by the broker/money launderer. The two parties would then confirm that this serial number matched the photograph of the dollar bill possessed by the person picking up the cash.

11. The money launderer broker arranged numerous such transactions with UC-1. On September 23, 2016, the money launderer broker reached out on Blackberry pin to pin to UC-1 and stated that he had a money pick up for "200," referring to $200,000 in Ohio for a 3.5 percent commission. UC-1 accepted the contract. UC-1 provided to the money launderer a telephone number of the courier (in this investigation, an undercover agent, hereinafter referred to as UC-2)

and the serial number F11592031L on a one dollar bill. A man, later identified as Moises Gonzalez, Jr. called UC-2 to arrange the specifics of the delivery of money in Dayton, Ohio. The designated location was a parking lot at 7767 Troy Pike Rd. in the greater Dayton, Ohio area. UC-2 placed Moises Gonzalez in contact with UC-3 for the actual transaction. On September 29, 2016, Gonzalez called UC-3 and stated there was someone he did not like in the designated location. The two agreed to change locations to a nearby parking lot at 8301 Troy Pike Rd. Gonzalez arrived in a blue BMW with Georgia license plates driven by an African American male identified as Jason Thomas. Gonzalez met with UC-3. Gonzalez handed a black and green backpack to UC-3. He stated it contained 4 packages of "30" and 2 of "40" totaling "200" (i.e. $200,000). Gonzalez then asked to see the photograph of the specific dollar bill with the serial number. UC-3 showed Gonzalez this photograph of the serial number on his cellular telephone. Gonzalez took a picture of it. Gonzalez then left with Jason Thomas. The money totaled $199,940.00.

12. UC-1 was informed of the delivery of the money. UC-1 in turn told the money launderer broker of the delivery of the cash. The broker/money launderer directed that the money (minus the 3.5 percent commission) be sent to:

(a) Acct # 7872229 belonging to "Classic Wholesale Inc., 11448 Harry Hines Blvd., Dallas, TX" at One World Bank in the amount of $17,000.

(b) Acct # 898080319415 belonging to JBP Corporation, 8275 Shadow Wood Blvd. Coral Springs, Fl. 33071 at Blank of America in the amount of $15,000.

(c) Acct # 632867680 belonging to Perfume Price Miami Inc., 2501 NW 34th Place, Pompano Beach, Florida at Chase Bank in the amount of $9,000.

(d) Acct # 1142991 belonging to American National Rags Co., 7413 Mesa Drive, Houston, Texas 77028, at East West Bank in the amount of $140,000.

(e) Acct #874320096 belonging to Perfume Distributors Inc., 2300 Marcus Avenue, New Hyde Park, NY 11042 at Chase Bank;

(f) Acct # 898080456200 belonging to Paquetes y programas Inc., at 682 NW 170 Terrace, Pembroke Pines, FL 33028

These transfers occurred.

13. Later on September 29, 2016, the money launderer broker told UC-1 that there was an additional "200" referring to $200,000 that needed to be picked up in Ohio from the same person. On September 30, 2016, UC-3 spoke with Moises Gonzalex, Jr. to arrange the pick up this money at the Meijer Store off Exit 29 on Interstate I-70 in Englewood, Ohio. Gonzalez told UC-3 that he would not be at the meeting. Gonzalez stated the black male driving the blue BMW from the day before, identified by law enforcement as Jason Thomas, would drop off the money.

14. Law enforcement observed the blue BMW with Georgia license plates exiting I-70 at Exit 29. An Ohio State Highway Patrol Officer conducted a traffic stop on the blue BMW driven by Jason Thomas for a traffic violation. A canine conducted a free air sniff of the blue BMW. The canine alerted for the presence of the smell of illegal narcotics. A search of the blue BMW revealed a blue Adidas bag that contained a large amount of US currency wrapped in

cellophane. The money totaled $205,050. The money was seized. Law enforcement also seized two cellular telephones from the vehicle including a white Apple iPhone with a gold cover (Target Device #1) as well as a black Blackberry cellular telephone model REY21CW (Target Device #2).

15. UC-1 texted the money launderer broker based in Colombia that Gonzalez had sent a black male (referring to Jason Thomas) to deliver the money and that Thomas had been stopped by police. The money launderer broker said that his associates could not locate Gonzalez or Thomas. The money launderer broker asked for details of the police stop, particularly whether the officer who conducted the stop was uniformed or wearing plain clothes.

16. Based on my training, experience, and knowledge of the case, the money laundering organization based in Colombia communicated with each other via cellular telephone, often via Blackberry pin-to-pin. The organization also communicated with couriers in the United States via cellular telephone. Indeed, several members of the money laundering organization communicated directly with undercover agents.

17. Target Device #1 and Target Device #2 are currently in the lawful possession of the **DEA**. As related above, the Devices came into the **DEA**'s possession in the following way: seized incident to arrest. Therefore, while the **DEA** might already have all necessary authority to examine the Device, your Affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

18. The Devices are currently in storage at the Dayton Residence Office, Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, OH. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the **DEA.**

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

26. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them

publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Steve Duteil
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me
on February 4, 2019:

Michael J. Neumann
UNITED STATES MAGISTRATE JUDGE